January 2013

Annual Security Refresher

Self-Study #1425

Los Alamos
NATIONAL LABORATORY
EST. 1943

Operated by Los Alamos National Security, LLC for the NNSA

Central Training-Institutional Training Services Group Leader
Richard J. Reynolds

MSS & Security Training Team Manager
Michael P. Benelli

Instructional Designer
Sharon S. Jennings

Technical Advisor
Robert L. Lopez

Editor/Compositor
Susan Basquin

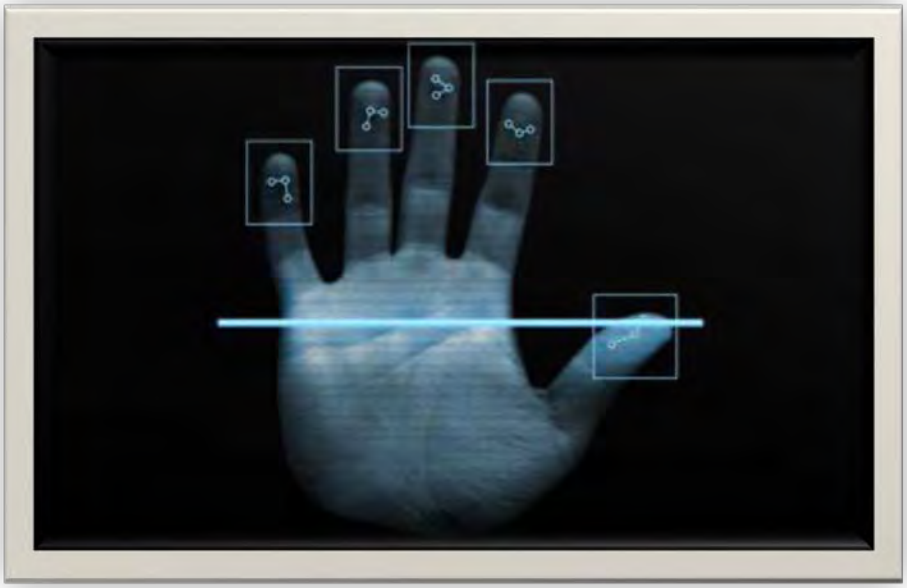
Course Number: 1425
January 2013
LA-UR-12-26887
Controlled Document Number: Annual_Security_Refresher_SS_1425, R8.1

This document was reviewed by a derivative classifier (DC) on December 4, 2012, and does not contain any classified information.

Contents

Introduction

Course Overview



This refresher training includes case studies based on security events or incidents. Each case study is followed by applicable security requirements and the applicable steps of the integrated safeguards and security management (ISSM) system. These case studies are based on real-life incidents that occurred at the Laboratory. However, the names of the employees who figure in the incidents have been changed.

Course Objectives

When you have completed this course, you will be able to

- identify requirements for reporting security incidents;
- identify events that Q- and L-cleared (or in process) workers must report to Personnel Security;
- identify requirements concerning access to security areas and property protection areas (“piggybacking” rule);
- identify requirements for controlled locks and keys;

Course Objectives—continued

- identify counterintelligence reporting requirements;
- identify the requirements for responding to a technical surveillance countermeasures (TSCM) incident;
- identify requirements for marking, accessing, and transporting classified matter;
- identify requirements for destroying classified matter;
- identify requirements for reproducing classified matter;
- identify requirements for reviewing technical information before it leaves the Laboratory;
- identify the policy concerning information in the public domain ("no comment" policy); and
- identify the requirements for receiving and transmitting controlled unclassified information (CUI).

Program Owner

This course was developed under the direction and technical oversight of the Security Integration Group, the functional program owner for this training.

Target Audience

This course is required for all L- and Q-cleared workers and uncleared workers when assigned by a line manager.

Credit

Credit for this course in the UTrain Learning Management System can be received two ways—completing the course or testing out:

- Completing the course does not require taking a quiz. After reading the material, click on the link at the end of the course to get credit.
- Testing out of the course requires a minimum score of 80 percent. Testing out can be completed at a proctor station or online with a CRYPTOCard® with administrative access. **To test out,** log in to UTrain and complete the quiz for course item 52199.

Acronyms

ADSS	Associate Directorate for Safeguards and Security
CI	counterintelligence
CRD	confidential restricted data
CUI	controlled unclassified information
DC	derivative classifier
DOE	Department of Energy
DSO	deployed security officer
DWI	driving while intoxicated
FRD	formerly restricted data
ISSM	integrated safeguards and security management
LA	limited area
LA-UR	Los Alamos-unlimited release
LANL	Los Alamos National Laboratory
L&K	lock and key
NIST	National Institute of Standards and Technology
PPA	property protection area
RD	restricted data
RLM	responsible line manager
SIT	Security Incident Team
SNM	special nuclear material
SPL	security program lead
SRD	secret restricted data
TSCM	technical surveillance countermeasures
UCNI	unclassified controlled nuclear information

Section 1: Security Requirements—Reporting

Overview

Information about known or potential security vulnerabilities may be sensitive or classified. Workers must properly protect this information from unauthorized disclosure and immediately report any known or potential incident of security concern to the Security Incident Team (SIT) or a deployed security officer/security program lead (DSO/SPL), and their responsible line manager (RLM).

Objective

When you have completed this section, you will be able to

- identify requirements for reporting security incidents.

Case Study: Reporting Security Incidents

Carlos, a Q-cleared employee, works in a property protection area (PPA). He brings his personal cell phone into his office every day. On occasion he has to attend meetings in secured limited areas (LAs) and knows not to take his personal cell phone into those areas. One Monday Carlos had a meeting with Christine who works in a limited area. Twenty minutes into the meeting, Carlos realized he had mistakenly taken his personal cell phone in with him. Upon discovery, he immediately removed the device from the area. Previous meetings with Christine had involved classified conversations, however at this particular meeting there had been no classified conversations in the vicinity of the phone at the time of the incident.

When he returned to his office, he sent an email to his deployed security officer (DSO) reporting the incident. The DSO, who was on leave, did not see the email until she returned to work five days later. The DSO then reported the incident to the SIT. Because of the delay it became a reportable security incident.

Requirements

Reporting Incidents of Security Concern. Information about known or potential security vulnerabilities may be sensitive or classified. Workers must ensure that sensitive and classified information is properly protected from unauthorized disclosure. Workers must immediately report any known or potential incident of security concern to the following:

- **Security Incident Team:** The worker must first notify the SIT at 665-3505 or a **Deployed Security Officer/Security Program Lead (DSO/SPL)**
  - If during normal hours of operation the DSO or SPL cannot be contacted, the worker must immediately notify the SIT directly or contact another DSO or SPL;
  - Outside normal hours of operation (7 a.m. to 5 p.m.), workers must immediately report known or potential incidents of security concern to the Associate Directorate for Safeguards and Security (ADSS) on-call duty officer at 699-4094 (cell) or 949-0156 (pager);

    Note: *If an incident of security concern is discovered outside the normal hours of operation and the on-call duty officer is notified, the worker has met the requirement to report the incident to a SIT representative.*

  and the

- **Responsible Line Manager (RLM)**
  The worker should notify a designated alternate or another manager in the management chain if
  - the responsible line manager (RLM) cannot be notified immediately, or
  - the RLM is not properly cleared to receive detailed information about the incident of security concern.

Note: *Workers must report known or potential incidents of security concern directly to the SIT representative or a DSO/SPL and their RLM. Reports must* ***not*** *be made through voice mail or email.*

Note: *Serious safety hazards or security risks may prevent workers from reporting a known or potential incident of security concern immediately. Workers must report as soon as they can do so safely and securely.*

For more detailed information on these requirements, please go to https://policy.lanl.gov/, *Reporting Known and Potential Incidents of Security Concern.*

ISSM Focus

Analyze the Security Risk and Develop and Implement Security Controls. Before work is performed, the associated security risks must be analyzed and security standards and requirements implemented to protect security interests.

Carlos should have immediately reported the incident to the SIT or DSO/SPL (and his RLM) instead of emailing the DSO. Do not email or use other unsecure forms of communication, e.g. voice mail, to provide information about an incident. Also, delayed reporting could have exacerbated the situation, especially if classified information had been involved.

Routinely bringing his personal cell phone to work resulted in Carlos' carrying the cell phone into the limited area. Carlos thought he would always remember to remove his cell phone before entering limited areas but clearly he did not. Had he analyzed the situation, he would not have brought the cell phone into the limited area.

Caution: *Cell phones can be remotely activated and turned into listening devices without the owner ever knowing.*

Section 2: Personnel Security

Overview

Workers are required to follow certain security guidelines while possessing a clearance or when in the process of gaining a clearance, and when on extended leave.

The Personnel Security Group ensures that granting an individual access to classified matter and/or special nuclear material (SNM) does not endanger common defense and security, and is clearly consistent with the national interest.

Objectives

When you have completed this section, you will be able to

- identify events that Q- and L-cleared (or in process) workers must report to Personnel Security, and

Case Study: Security Clearance Reporting

Sergio is a Q-cleared worker who was recently arrested for driving while intoxicated (DWI). His lawyer told him not to report the incident to LANL because he had not been convicted in a court of law. Based on his lawyer's advice, Sergio neglected to report the incident to Personnel Security. The Laboratory ultimately discovered this information because arrests are published in newspapers along with mug shots. Sergio now had two issues that needed to be mitigated. The first one was the DWI that may have been easily dealt with assuming there were no associated alcohol abuse issues. The second issue was his failure to report the arrest as required by the DOE.

Requirements

Security Clearance and Maintaining a Clearance. A worker who holds a clearance or is in the process of gaining a clearance is required to report to Personnel Security within ONE working day any arrests, criminal charges (including charges that are dismissed), or detentions by federal, state, or other law-enforcement authorities for violations of law within or outside the United States. A traffic violation for which a fine of up to $300 was imposed does not need to be reported.

Note: *All alcohol- or drug-related traffic violations must be reported, regardless of fine.*

Other reporting requirements include personal or business-related bankruptcy, garnishment of wages, legal actions effected for name change, change in citizenship, and many others.

For more detailed information on these requirements, please go to https://policy.lanl.gov/, *Security Clearances*.

ISSM Focus

Analyze the Security Risk. Although Sergio wasn't performing work, he should have analyzed the impact on maintaining his security clearance (and possibly his job) and made sure he was following LANL and DOE requirements. If he had appropriately reported the DWI, his credibility would not have been in question.

The DOE evaluates issues that arise with clearance holders on a daily basis. Workers often assume incorrectly that as long as they win the case in court, the DOE will not have an issue with the arrest. The DOE is not the criminal court system. The courts are attempting to determine if a person is guilty beyond a reasonable doubt. The DOE is trying to decide if the worker can be trusted with information that is critical to national security. One of the ways that the DOE can help make this determination is to know that the worker will report incidents as they arise. Once a worker fails to adhere to the rules regarding the reporting of information, the DOE becomes concerned and begins to ask the question, *Can we trust this person?*

Section 3: Physical Security

Overview

This section provides some case studies that focus on Physical Security requirements governing personnel who work in areas that have classified matter, including but not limited to prohibited articles on Lab property, access requirements for security areas and property protection areas (specifically the “piggybacking” rule), and control of locks and keys.

Objectives

When you have completed this section, you will be able to

- identify requirements concerning access to security areas and property protection areas (“piggybacking” rule), and
- identify requirements for controlled locks and keys.

Case Study: Access—Piggybacking Rule

Paul, a Q-cleared worker, was already running late for work when he realized that his badge was not in its usual place. Paul had several deadlines looming, so he felt pressure to get to work on time. Deciding to resume his search for his badge at lunchtime, Paul walked to his building, a PPA, and waited for someone to let him in. George arrived soon and since George and Paul knew each other by sight, George allowed Paul to piggyback into the building.

Once inside, they parted ways. Martin, a DSO conducting a security walk-around, noticed that Paul was not wearing a badge. Martin asked Paul about his badge. Paul replied he had been "escorted" in that morning and was intending soon to obtain a temporary badge from the Badge Office. Martin immediately escorted Paul out of the building and contacted the SIT to report the incident.

Requirements

Piggybacking. Piggybacking is not allowed in PPAs or security areas where an active security badge reader system controls access.

Using a Badge. All badge holders, including workers or official visitors, must wear their badge, photo side out and above the waist on the front side of the body, *at all times* while on Laboratory property.

For more detailed information on these requirements, please go to https://policy.lanl.gov/, *Security Areas, Property Protection Areas, and General Access Areas* and *Security Badges*.

ISSM Focus

Analyze the Security Risk and Perform Work within Security Controls. Access to PPAs and security areas is limited to authorized workers based on need-to-know, operational requirements, and mission needs. Piggybacking is a practice in which a worker with the required clearance to access an area allows another worker with an appropriate badge and a need-to-know to enter the area without using automated access controls (such as badge readers or palm readers).

ISSM Focus—continued

Although George knew Paul, he should not have let Paul into the building (even if Paul had his badge and, let's say, it wasn't working on the badge reader). George had no idea if Paul's access status had changed and by letting him in, badge or no badge, George was responsible for Paul having access to an area where he possibly was no longer allowed and, to make it worse, he allowed him in without a badge.

Paul should have known that piggybacking isn't allowed and he absolutely had to know that being in a Lab building without a badge isn't allowed either. But possibly due to the stress of running late and work deadlines, he ignored the rules. Be aware that stress of any kind can have a major effect on human error.

Case Study: Security Locks and Keys

Yuri, a Q-cleared worker, was issued a Level III key (see explanation for Level III keys under Requirements) to an electronics lab in a LANL limited area where he was conducting experiments utilizing material classified as secret restricted data (SRD). Bruce, an L-cleared worker in the same group as Yuri, asked Yuri if he could borrow his key to the electronics lab since his supervisor had forgotten to issue him one. Because Yuri knew Bruce was in the same group and because the next day was Yuri's Friday off, he gave his key to Bruce.

On Friday, Bruce used the borrowed key to enter the electronics lab to get an oscilloscope for use in another lab. As he entered the lab, Bruce interrupted other Q-cleared workers doing some testing on material that was classified SRD. Bruce's L clearance did not allow him access to this classification of work, so this incident represented a potential unauthorized disclosure and was immediately reported to the SIT.

Requirements

Security Locks and Keys (Use of Level III Keys). Keys, padlocks, and cores must be protected and controlled based on their level (I, II, III, or IV). Level III keys must be under the direct control of the key recipient (kept on the recipient's person or stored in a desk drawer or cabinet under the recipient's control). If taken off-site, Level III keys must be protected in the same manner as the DOE security badge. Do not lend an assigned key to another worker without written authorization from the lock and key (L&K) coordinator.

Level III keys, cores, and padlocks are used to prevent unauthorized access to limited areas, to Category IV SNM, and to government property that, if lost, would adversely affect Laboratory security or operations. Level III keys are used in conjunction with other security controls for the interior doors (e.g., office doors) in buildings and office areas where workers are permitted to leave classified matter temporarily unattended in accordance with an approved security plan.

***Note**: Return all issued keys to the L&K custodian before transferring to another organization or terminating employment.*

For more detail information on these requirements, please go to https://policy.lanl.gov/, *Security Locks and Keys*.

ISSM Focus

Analyze the Security Risk and Perform Work within Security Controls. Although the group correctly reported this potential security incident to the SIT, Yuri should not have lent his key to any other worker without authorization by the L&K coordinator. If Yuri had contacted the coordinator, the responsible line manager (RLM) would have been asked to determine whether Bruce had the proper clearance and need-to-know for unescorted entry into this area. The RLM would have identified that there was a classified project in this lab and that only Q-cleared workers could be issued a key to this lab.

What's new in Physical Security?
All vehicles entering LANL at the East Jemez Vehicle Access Portal (VAP) during nonwork hours (between 7 p.m. and 5 a.m. on weekdays and all day on weekends) will be funneled into the center lane (Lane #4). All other VAP lanes will be closed during nonwork hours. Drivers must stop at the center lane guard post and proceed only upon verbal or hand signal direction from the Protective Force officer.

Section 4: Counterintelligence and Technical Surveillance Countermeasures

Overview

The Laboratory's vital national security role can be compromised by intentional acts of hostile intelligence services or through inadvertent behavior of its employees. The mission of the LANL Counterintelligence (CI) program is to protect the Laboratory and its employees from efforts by foreign intelligence services and terrorist entities to acquire sensitive and/or classified information.

Technical surveillance countermeasures (TSCM) are techniques to detect and nullify a wide variety of technologies that are used to obtain unauthorized access to sensitive or classified information. In other words, they locate electronic or technological "bugs."

Objectives

When you have completed this section, you will be able to

- identify counterintelligence reporting requirements, and
- identify the requirements for responding to a TSCM incident.

Case Study: Counterintelligence Reporting Requirements

Four LANL employees recently traveled to California to participate in a scientific conference. While there, two foreign nationals, who were also attending the conference, approached the LANL employees at the hotel lounge and began asking vague and open-ended questions regarding their programs. One of the questions, for example, went something like this: "We know a guy… what was his name who wrote the big codes in LMNO Division?" At the same time the other individual proceeded to take pictures of the LANL team. One of the LANL employees felt very uncomfortable and asked to see the camera. He then proceeded to delete the pictures. The foreign nationals made no comment and quickly left the lounge.

Case Study: Counterintelligence Reporting Requirements—continued

At a banquet the following evening, the same foreign nationals singled out one of the LANL employees who had given a presentation earlier in the day. They began asking questions, which made the LANL employee uncomfortable because they were being quite persistent and also because they appeared to know personal information about the employee. The LANL employee finally told them they could find in open literature the information they were interested in. The two eventually left the banquet.

When the LANL employees returned to work, they reported what happened to the CI Program Office, as required.

Requirements

Counterintelligence (CI) Reporting Requirements and Individual Reporting Requirements. Workers must report the following occurences to the CI Program of the Office of Counterintelligence:

- any actions the worker has encountered while on travel that he or she believes to be suspicious or provocative;
- any attempts by unauthorized persons to gain access to sensitive or classified information; and
- professional contacts and relationships with sensitive country foreign nationals, whether they occur at the Laboratory or outside the workplace.

Other reporting requirements include all unofficial travel to any sensitive country, substantive personal relationships with foreign nationals of sensitive countries, business transactions with citizens of sensitive countries who are not lawful permanent residents of the United States, and many more.

For more detailed information on these requirements please go to https://policy.lanl.gov/, *Counterintelligence Reporting Requirements.*

ISSM Focus

Analyze the Security Risk. The LANL employees followed the correct steps to take when encountering suspicious attempts to obtain information. LANL employees do not have to travel abroad to be approached by people seeking information about what they do. Lab employees must always be aware that others know who they are and what they do. Congratulations to the Lab employees who did their part in protecting our national security information.

Case Study: Responding to a TSCM Incident

Some of the water pipes in a secure facility had been leaking in the ceiling, causing water to drip into the building's conference room. A facilities service request was made, and a team of uncleared workers was dispatched to fix the pipes. They were provided an escort and worked in the conference room for one day. In performing their work they spent the majority of their time above the ceiling tiles and out of view of the escort.

The next day, during a team meeting where some classified information was discussed, Lionel, the team leader, heard a strange sound coming from one of the vents when the air conditioning switched on. It sounded as if something were hitting the inside of the conduit as the air went by. After the meeting concluded, Lionel decided to conduct a closer inspection of the conduit and to his surprise saw what appeared to be wires with an object attached at the end. He immediately vacated the room, locked the door, walked over to his group leader's office, and informed his group leader of the situation. Knowing the requirements, the group leader immediately reported the situation to the TSCM Program Office and had Lionel go back to the room and guard the door so that no one else would enter.

Requirements

TSCM Incident Response. Discovery of a technical surveillance device or system or the suspicion of the existence of a device or system in any facility must be reported immediately to the Technical Surveillance Countermeasures Program Office. The reporting of any discovery or suspicion of a technical surveillance device or system must be made outside the facility where the suspected surveillance exists, preferably in person. The TSCM Program will ensure that appropriate protection and preservation is afforded to the suspected technical surveillance system or device and will complete any additional reporting requirements.

For more detailed information on these requirements, please contact the *Technical Surveillance Countermeasures Program Office*.

ISSM Focus

Analyze the Security Risk and Develop and Implement Security Controls. Lionel did the right thing by leaving the room, locking the door, and reporting the situation to his group leader in person. He was so surprised by what he found that he didn't stop to think about protecting the room. Fortunately his group leader remembered what to do and contacted the TSCM Program Office.

When he heard the noise he assumed, as most of us would, that something had come loose and he continued the meeting. Now he knows he should have discreetly stopped any classified or sensitive discussions and ended the meeting.

ISSM Focus—continued

If you discover a technical surveillance device or system or suspect the existence of a device or system in any facility, follow these steps:

1. Go about your activities as if nothing special has happened. Make sure to censor your conversation if sensitive or classified information was to be discussed.
2. Do not touch the device.
3. Do not discuss the device.
4. After the meeting, lock the room and do not let anyone enter the room. If possible, someone should stay by the door to ensure the integrity of the room.
5. Leave your secure area and contact the TSCM Program Office. If you are using an unsecure phone, do not discuss the details of the device.
6. Meet with TSCM personnel and show them where the device is located.
7. TSCM personnel will contact all other individuals who need to be informed of the situation.

These steps are very important in ensuring that the TSCM Program Office has all available opportunities to neutralize a potentially hostile technical penetration. If the device in this situation were indeed a microphone put in place for the purpose of clandestine surveillance, any sudden abnormal behavior or discussion of the device could tip off the individual sitting at the listening post that his or her device had been discovered. This would make a successful investigation very difficult.

Another aspect to keep in mind is that if your area has been targeted for exploitation, there could very well be more than one device located in your secure area. It is for this reason that it is important that you do not discuss the device in your secure area but rather call TSCM from a phone located outside your secure area.

Section 5: Classified Matter Protection and Control

Overview

The Classified Matter Protection and Control program exists to ensure proper use and protection of classified matter. This section provides some case studies that focus on security requirements governing personnel who work with classified matter.

Objectives

When you have completed this section, you will be able to

- identify requirements for marking, accessing, and transporting classified matter;
- identify requirements for destroying classified matter; and
- recognize requirements for reproducing classified matter.

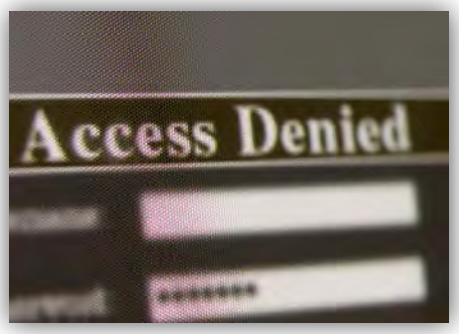
Case Study: Marking, Accessing, and Transporting Classified Matter

Xavier, a Q-cleared worker, was employed in a property protection area. As part of a security incident into improper transmission of classified information, Xavier worked with the SIT, a DSO, and cyber security personnel to sanitize the work area of classified matter.

A week after completing the task, Xavier remembered he had a compact disc that contained confidential restricted data (CRD) that he had forgotten to mark. In a hurry to leave for a doctor's appointment, Xavier retrieved the CD and asked Marta, a Q-cleared worker, if she would take the CD to Pat, who had provided the information on the CD. Marta asked Xavier if the CD was classified, to which Xavier replied, "I'm not sure."

Marta said she would not take a potentially classified CD because she might not have the proper clearance and need-to-know. Marta could not find Pat and told Xavier, and he again asked her to take the CD since he had to leave. Marta again refused. Xavier stated he would take the CD to his doctor's appointment and return later. Marta told Xavier he could not take potentially classified information to a doctor's appointment and then she attempted to locate Pat once again. After finding Xavier had left, and assuming, based on what he had told her, that he had taken the CD, Marta reported the situation to the SIT and the RLM.

However, before leaving, Xavier did give the CD to another coworker, Shirley. Shirley immediately notified the SIT and the RLM that she accepted a potentially classified CD from Xavier (for Pat) because she did not think Xavier was in any state of mind to properly protect the data.



Requirements

Marking Classified Matter. Compact discs containing classified matter are required to be marked with the classification level, classification category (if restricted data [RD] or formerly restricted data [FRD]), unique identification number/barcode, if required, and caveats, as applicable.

Access Requirements for Classified Matter. Access to classified matter **must** be limited to workers who possess appropriate access authorization (i.e., security clearance), any formal access approvals (i.e., Sigma authorities, sensitive compartmented information [SCI] clearance, etc.) and who have a need-to-know for the performance of official duties.

***Note**: In an emergency situation involving imminent threat to life or national security, individuals who are not otherwise routinely eligible for access to classified matter or information may be granted access.*

Transporting Classified Matter. Workers hand carrying classified matter must

- have the required access authorization or clearance level for the information;
- be aware that they are carrying classified matter so it can be protected and controlled;
- travel directly to the recipient's location without making any stops (i.e., do not stop in the kitchen, the break room, to visit with a colleague, etc.);
- verify the recipient's clearance and need-to-know before transferring classified matter;
- inform the recipient that the document is classified and cannot be left unattended; and
- ensure that the recipient signs and dates the receipt, if required.

For more detailed information on these requirements, please go to https://policy.lanl.gov/, *Classified Matter Protection and Control Handbook*.

ISSM Focus

Define the Scope of Work and Analyze the Security Risk. Improperly marked, secured, packaged, or transported classified data is a risk of unauthorized disclosure.

Given his assistance in the recent security incident involving improper handling of classified matter by another party, Xavier should have known the requirements. Had he worked to identify potential requirements, analyzed possible security risks, and therefore identified opportunities to improve work execution, he would not have improperly handled classified matter.

Personal issues (in this case a possible medical condition) can significantly affect your judgment (for example, Xavier seemed confused about the classification of the data and also stated he was going to take it with him to his doctor's appointment). Let a coworker or your RLM know if you are undergoing a stressor that could affect your judgment. Ask for help.

If you notice a coworker behaving in an out-of-the-ordinary manner and in a way that could put classified matter at risk, notify the SIT or DSO/SPL and RLM immediately. If necessary, issue a stop work order. In this case, Marta and Shirley did the appropriate thing by immediately notifying the SIT and the RLM.

Case Study: Destroying Classified Matter

Lisa, a Q-cleared worker, was going through her safe and determined she could destroy a couple of classified documents. She took her classified documents (with cover sheets attached) to the group office to shred in an approved classified shredder. Lisa shredded her documents. After the shredder stopped running, she opened the shredder door to inspect the shred residue. To Lisa's surprise she found large pieces of paper rather than the typical shred residue. Lisa immediately notified the group administrator, Sarah, of the mechanical problem. Lisa and Sarah removed the shred bag and placed it in a safe drawer. Lisa then called the SIT and the RLM to notify them of the shredder malfunction.

Sarah immediately unplugged the shredder and placed a sign on the unit indicating that it was out of service. Sarah then called to schedule maintenance of the shredder.

Requirements

Destroying Classified Matter. Classified matter **must** be destroyed beyond recognition to preclude subsequent access to any classified or sensitive information or other matter. Each time material is destroyed, the residue must be inspected to ensure that it meets requirements.

If a worker discovers that a shredder is producing residue that does not meet the required specification, the worker must remove the unit from service by unplugging the unit, remove the residue bag and place it in a certified vault, closed area, or safe, and report the situation to the SIT or DSO/SPL and the RLM. Additionally, the worker must label the unit to indicate it is malfunctioning and then call for service.

For more detailed information on these requirements, please go to https://policy.lanl.gov/, *Classified Matter Protection and Control Handbook*.

ISSM Focus

Perform Work within Security Controls. Had Lisa not checked the shred residue after destroying her classified documents, it is unknown what could have happened with those large pieces of classified paper. A potential unauthorized disclosure could have occurred had someone without proper need-to-know come across the document pieces.

Both Lisa and Sarah followed the necessary steps when destroying classified documents and discovering that the unit did not function appropriately. Not all security incidents result from human error but rather can result from failure of equipment.

Case Study: Reproduction of Classified Matter

Elvis had just copied several classified documents regarding his project for a presentation the next day. While collecting the material from the classified copier, he dropped several pages on the floor, some of which ended up behind the copier.

Case Study: Reproduction of Classified Matter—continued

Upon moving the copier, Elvis noticed that a transparency was wedged behind it. He picked up the transparency along with his papers, locked the jumble of documents in his safe, and left for the day. The next morning, Elvis studied the transparency more closely and realized it contained SRD. Elvis immediately contacted the SIT and then his RLM to report his discovery of the classified transparency.

Requirements

Access. Protect classified matter from unauthorized physical, visual, or aural access and ensure that classified matter is attended or stored in an approved security container.

Reproduction. Protect and control the classified matter being reproduced as well as any classified matter resulting from the reproduction process. Ensure that no classified pages remain in or around the reproduction machine after use.

For more detailed information on these requirements, please go to https://policy.lanl.gov/, *Classified Matter Protection and Control Handbook*.

ISSM Focus

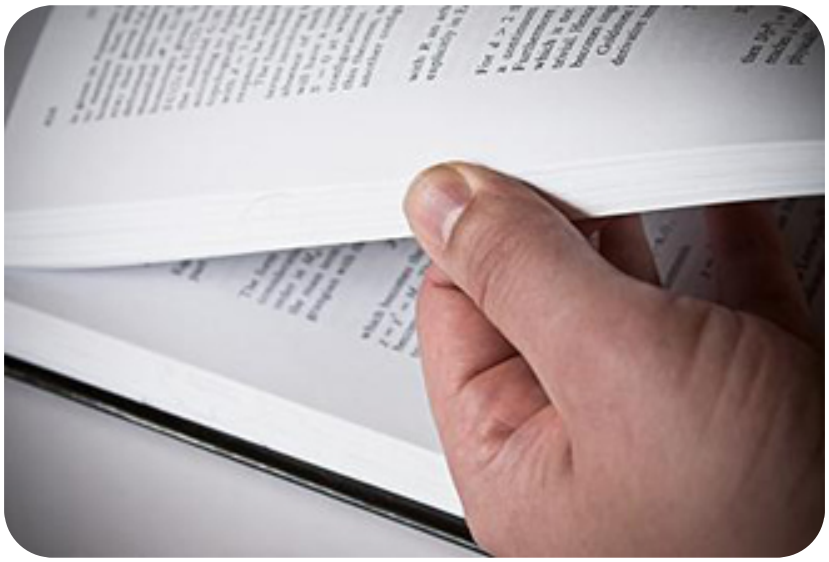
Perform Work within Security Controls. Classified information requires constant protection. Someone who did not have the need-to-know could have accessed the classified transparency wedged behind the classified copier. Classified matter must never be left unattended.

If it appears that a piece of paper or transparency with classified information has jammed or been lost in or behind a copier, one must make every effort to protect the equipment until the missing pages are retrieved. Those who photocopy classified matter must pay attention to how many pages to expect at the copier and then account for every page when the copy job is complete.

Anyone who finds classified or potentially classified matter is required to protect it. Elvis was right to secure what he found with the rest of his documents even though he was not sure at first glance what the transparency contained. Once he realized the transparency was classified, he did the right thing by contacting the SIT and his RLM to report the potential incident.

Section 6: Classification and Controlled Unclassified Information

Overview



This section provides some case studies that focus on requirements for the classification of documents and requirements for protecting information that, while not classified, falls under one or more categories of information requiring protection from unauthorized dissemination.

Objectives

When you have completed this section, you will be able to

- identify requirements for reviewing technical information before it leaves the Laboratory,
- identify the policy concerning information in the public domain ("no comment" policy), and
- identify the requirements for receiving and transmitting controlled unclassified information (CUI).

Case Study: Review of Matter and the Release of Technical Information

Jacob is getting worried. An important conference is one week away and he still hasn't finished the presentation he will be giving at the opening session. In order to save time, Jacob decides to skip submitting the presentation for an LA-UR (Los Alamos-unlimited release) number. He is confident that there's nothing classified in the paper. He'll submit it after the fact and all should be fine.

After the conference, Jacob submits the paper for review. The next day, he receives a phone call from the Classification Group; they would like him to come over and discuss his paper. Jacob learns that he has included a piece of information that is confidential restricted data (CRD), and that he has made an unauthorized disclosure of classified information. The Security Incident Team (SIT) is called, and Jacob receives a security infraction for failure to have his paper reviewed by a derivative classifier (DC) before release.

Requirements

Review of Matter. Laboratory workers must ensure that documents or materials they generate are reviewed for classification and sensitive information.

Technical Information Release. All technical information intended for widespread distribution or public release must be submitted to the Classification Group for review before leaving the Laboratory. This requirement applies to

- formal reports;
- journal articles;
- abstracts;
- viewgraphs;
- conference papers;
- books or book chapters; and
- other documents intended for public release, including safety analysis reports, environmental reports, regulatory compliance documents, etc.

For more detailed information on these requirements, please go to https://policy.lanl.gov/, *Classification of Matter; Review and Approval of Scientific and Technical Information (STI).*

ISSM Focus

Perform Work within Security Controls. Jacob should have submitted the document for a classification review before release, but possibly because of his stress over the upcoming deadline and absolute confidence it was unclassified, he ignored the rules. Be aware that stress of any kind can have a major effect on human error, and even though you may think you know the information well enough to determine classification, you may not, as in this case. Always submit for review.

Case Study: "No Comment" Policy

Jack asked his uncleared student, Susie, to provide some "filler" information for an unclassified briefing he was planning to present to a group of new hires. Using her LANL laptop, Susie diligently researched articles and websites for information that would be useful for the presentation. After compiling the information, Susie then added it to the presentation and emailed it to Jack. After looking it over, Jack realized that some of the information Susie provided might be classified. He took the presentation to the Classification Group, where portions of what she found were determined to be secret restricted data (SRD). Jack immediately reported the situation to the SIT and his RLM.

It was easy to isolate and sanitize Jack's computer. But Susie, who was uncleared, could not be told of the contamination because the fact that her computer was contaminated was itself classified information. Cyber Security developed a ruse to sanitize Susie's LANL computer without letting her know what was being done or why. They discovered that Susie had emailed the presentation to her personal account. Security officials requested that the DOE expedite Susie's clearance so that her personal computer could be sanitized. After receiving her clearance, Susie was notified of the incident, which allowed her to assist Cyber Security in sanitizing her home computer. In accordance with DOE's no comment policy, no attempt was made to locate the classified information on the Internet service provider servers.

Requirements

"No Comment" Policy. Information that is classified by the United States government may on occasion appear in the public domain, in print, or in broadcast media reports. However, such information in the open literature or any other form of communication does not automatically make it unclassified and requires workers to ensure that

- the information is not used or referred to in an unclassified setting;
- no comment is made in any way regarding the accuracy, classification, or technical merit of such information; and
- due care is exercised when discussing such information, even among fellow employees who may not possess the required clearance and/or need-to-know.

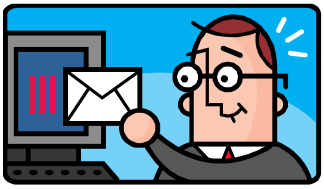
If such information is classified, that fact itself requires protection as classified information.

For more detailed information on these requirements, please go to https://policy.lanl.gov/, *Classification of Matter*.

ISSM Focus

Analyze the Security Risk and Perform Work within Security Controls. Jack should have known that classified information could be on the Internet and should have conducted the research himself instead of asking Susie (an uncleared person and someone unfamiliar with the classification of the information she was gathering). If he had analyzed the risk and performed the work within security controls, i.e., had not copied the classified information onto a computer, he would have prevented this incident. Fortunately he discovered the classified information before using it in the briefing to the new hires.

Case Study: Receiving and Transmitting Controlled Unclassified Information (CUI)



Tom was instructed to get a package of drawings to a contracting firm (working on a Lab project) by the end of the week. Tom was off work on Friday, so that meant he had to finish and send off the package by the end of the day on Thursday. All was going well until Tom noticed that he was missing a drawing, one that would take time to get. It took a while, but he finally got the missing drawing, did a quick check to make sure he had everything, put the documents together as an email attachment, and sent them off just in time. On Monday, Tom's supervisor called to tell him that one of the drawings he sent was labeled unclassified controlled nuclear information (UCNI); Tom's quick check had missed it. The email with the attachments was sent outside the Laboratory's yellow network firewall.

Requirements

Receiving and Transmitting Controlled Unclassified Information (CUI); Unclassified Controlled Nuclear Information (UCNI). When transmitted electronically outside LANL, UCNI must be encrypted with National Institute of Standards and Technology (NIST)-validated encryption software. Emails with UCNI attachments are considered transmittal documents and must be marked as such. When UCNI is transmitted within the LANL yellow network, no encryption is required but it is suggested. It is the sender's responsibility to ensure that the recipient understands the sensitivity of the information and the requirements for protecting that information.

Workers must follow all requirements pertaining to the identification, protection, and control of CUI.

For more detailed information on these requirements, please go to https://policy.lanl.gov/, *Controlled Unclassified Information*.

ISSM Focus

Analyze the Security Risk and Perform Work within Security Controls. Tom felt the pressure of the deadline to get the information emailed and therefore missed seeing the UCNI drawing. Be aware that stress of any kind can have a major effect on human error.

Resources

The **Security Help Desk** provides assistance for security-related issues. Call 665-2002.

The **Security Incident Team (SIT)** can be reached at 665-3505 (reports must not be made through voice mail or e-mail). The **ADSS on-call duty officer** can be reached at 699-4094 (cell) or 949-0156 (pager) outside of normal hours of operation. Normal hours of operation are 7 a.m. to 5 p.m.

The **Technical Surveillance Countermeasures Team** provides technical support and can be reached at 665-3409.

Security program leads (SPLs) provide security expertise and serve as a single point of contact on security matters for directorate personnel.

Deployed security officers (DSOs) coordinate and oversee all division security activities. DSOs are available to work with any security-related issue.

Organizational computer security representatives (OCSRs) are the main point of contact for all cyber security activities for unclassified and classified systems.

Cyber systems security officers (CSSOs) are responsible for ensuring that protective measures are installed and that operational security is maintained for one or more specific classified information systems and/or networks.

Institutional procedures serve to guide LANL workers on the requirements that pertain to LANL-specific operations. These procedures ensure compliance with DOE directives.

The **Security website** provides information on all security-related topics, including the following topics:

- Protecting information
- Personnel security
- Cyber security
- Nuclear materials
- Facility security
- Integrated security

Safeguards and Security Procedures

- Classification of Matter, P204-3
- Classified Matter Protection and Control Handbook, P204-2
- Controlled Unclassified Information, P204-1

Resources—continued

- Counterintelligence Reporting Requirements, P203-4
- Integrated Safeguards and Security Management, SD-200
- Management of Classified Parts, P821-2
- Nuclear Material Control and Accountability, PD 205
- Controlled Articles, P217
- Prohibited Articles, P202-5
- Reporting Known and Potential Incidents of Security Concern, P201-3
- Review and Approval of Scientific and Technical Information (SIT), P1022
- Security Areas, Property Protection Areas, and General Access Areas, P202-1
- Security Badges, P203-1
- Security Clearances, P203-2
- Security Locks and Keys, P202-4
- Vault and Closed Areas, P202-2

DOE Orders

- DOE Order 470.4B, Safeguards and Security Program
- DOE Order 471.6, Information Security
- DOE Order 472.2, Personnel Security
- DOE Order 475.1, Counterintelligence Program
- DOE Order 475.2A, Identifying Classified Information

Course Credit

To submit for credit for reading this document, click on the following URL:

http://ExTrain.lanl.gov/CreditRequest.aspx?Token=xS5MEb/O88kRp0KS3Gi05g~~